UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,608	03/28/2001	Virgil Dorin Gligor	068398/0104	1778

22428 7590 07/14/2005

FOLEY AND LARDNER
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/818,608	**Applicant(s)** GLIGOR ET AL.	
	Examiner Minh Dieu Nguyen	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-91* is/are pending in the application.

4a) Of the above claim(s) *52-60,65-70,75-80,87,88,90 and 91* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,26-28,34-36,49-51,61-64,71-74,81,86 and 89* is/are rejected.

7)☒ Claim(s) *7-25, 29-33, 37-48, 82-85* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *6/28, 7/24/01*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication dated March 21, 2005 with the election of group 1a (claims 1-51, 61-64, 71-74, 81-86 and 89).

Claims 1-51, 61-64, 71-74, 81-86 and 89 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6, 26, 34-36, 49, 61-64 and 71-74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (6,769,063) in view of Zeidler (4,423,287)

a) As to claims 1, 6, 36, 61, 63-64, 71 and 73-74, Kanda discloses a data transformation device in which the round function is so configured as to simultaneously meet the requirements of security and speedup to thereby ensure security and permit fast encryption processing without involving a substantial increases in the number of rounds (col. 6, lines 13-19) comprising the step of partitioning data into a plurality of data blocks (i.e. every 64-bit data is entered into the crypto device, Fig. 4, element 301); for each of the data blocks, performing a randomization function over the data block to create an input block of the same size as that of the data block, the input block not including a block identifier (Fig. 4, element 302; col. 9, lines 30-34); applying a pseudo-random function to each input block to create a plurality of enciphered blocks (Fig. 4, element 38.sub.0).

However Kanda does not disclose combining the plurality of enciphered blocks to create an authentication tag.

Zeidler discloses an encryption system with a message authentication code included along with the protected data elements in a message to be transmitted to the destination (col. 2, lines 10-17) comprising combining plurality of enciphered blocks to create an authentication tag (Fig. 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of creating an authentication tag in the system of Kanda as Zeidler teaches so as to protect information against alteration.

b) As to claims 2, 62 and 72, Kanda as modified discloses the pseudo-random function is a standard block cipher (col. 1, lines 18-30).

c) As to claim 3, Kanda as modified discloses each of the data blocks is l bits in length (every 64-bit data is entered into the crypto device, Fig. 4, element 301).

d) As to claims 4-5, Kanda as modified discloses creating a random vector block of l bits in length and performing a randomization function over the plurality of data blocks includes performing the randomization function over the random vector block (Fig. 4, element 302).

e) As to claims 26 and 49, Kanda as modified (see claims 6 and 36) Zeidler discloses the combination operation comprises a bitwise exclusive-or operation (see Zeidler, Fig. 13, element 168).

f) As to claims 34-35, Kanda as modified discloses performing a randomization function over the plurality of plaintext blocks and the random vector block is done concurrently for each plaintext block and the random vector block, and the plurality of plaintext blocks and the random vector block are concurrently presented to a plurality of block ciphers using a secret key (Fig. 4).

4. Claims 27-28 and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (6,769,063) in view of Zeidler (4,423,287) and further in view of Jones et al. (6,434,699).

As to claims 27 and 50, Kanda and Zeidler do not disclose addition modulo and as to claims 28 and 51, Kanda and Zeidler do not disclose subtraction modulo.

Jones discloses an encryption chip is programmable to process a variety of secret key and public key encryption algorithms comprising an addition and subtraction modulo (Fig. 15D).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having addition and subtraction modulo in the system of Kanda and Zeidler as Jones teaches so as to compute the authentication tag algorithms.

5. Claims 81, 86 and 89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (6,769,063) in view of Zeidler (4,423,287) and further in view of Bellare et al. (5,757,913).

As to method of claim 81, program code of claim 86 and system of claim 89, Kanda and Zeidler do not disclose partitioning the data into a plurality of data blocks further comprises data padding.

Bellare discloses a method and apparatus for data authentication in a data communication environment comprising the step of partitioning the data into a plurality of data blocks further comprises data padding (Fig. 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having data padding in the system of Kanda and Zeidler as Bellare teaches so as to make data block with the same size.

Allowable Subject Matter

6. Claims 7-25, 29-33, 37-48 and 82-85 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Kanda and Zeidler fails to anticipate or render the step of combining each of plaintext blocks and random vector block with a different corresponding element of a sequence of unpredictable elements to create a plurality of input blocks (claim 7).

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
7/7/05

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137